REMARKS

This is in response to the Office Action mailed on October 3, 2007. In that action, claims 1-29 were rejected under 35 U.S.C. §102(b) as being anticipated by Jancula, U.S. Publication No. 2002/0023208 A1 (hereinafter "Jancula"). In this response, claims 1, 9, 11 and 12 are amended. Claims 10 and 13 have are cancelled. The remaining claims are unchanged.

An interview was conducted with the Examiner on January 3, 2008. All of the independent claims and the amendments included herewith were discussed. No agreement was reached but the Examiner agreed to strongly consider the amendments and arguments included herewith.

INTRODUCTION

Jancula is directed to a method for enabling a third-party agent to securely access a customer's private personal and financial from a second party, preferably over the Internet. A security ticket is presented to the second party in order to verify the customer's consent to access the data. The second party only communicates the confidential information to the third party if the security ticket is found to be valid. The security ticket can include a preselected expiration time, beyond which it is invalid.

Jancula is also directed to a system wherein a customer interacts with an aggregator website, which in turns interacts with commerce websites. As discussed in paragraph 0054 of Jancula, the aggregator's website uses standard Internet software to access the commerce websites on behalf of the customer. The aggregator collects the customer's private data from the commerce websites and consolidates the data for access by the customer. The customer need only access the aggregator's website to view their consolidated private or confidential information obtained by the aggregator from the multiple commerce websites.

In contrast, embodiments of the present invention pertain to a communication protocol to be implemented between a software application and a service provider. The protocol generally involves downloading a long-lasting security certificate during the process of registering the software application. An access ticket, which is encrypted based at least in part on

information contained in the long-lasting certificate, is generated to enable to particular person (or particular class of persons) to access a particular service or services from the provider of services during a period of time within which the access ticket is valid. The scope of permissions, including assigned user classes, and duration of access can be configured or reconfigured by the host of the application software. Other embodiments of the present invention pertain to utilization of a similar protocol to enhance the security of peer-to-peer communication, for example, communication between two software applications over a public network.

CLAIMS 1-9, 11

With the present response, claim 1 has been amended to clarify that the claim step of "applying a collection of security privileges to a set of authentication credentials to determine if a user is authorized to carry out the request," more specifically comprises "applying based at least in part upon a role-based determination that involves referencing a record that assigns access privileges to various roles that can be assumed by the user." It is respectfully submitted that Jancula does not teach or suggest a role-based determination involving a record that assigns access privileges to various roles that can be assumed by the user. The Office Action on page 6 asserts that paragraphs 0057-0058 and 0071-0075 of Jancula teach applying a collection of security privileges. Although paragraph 0074 shows that a customer will inform the aggregator about each of his or her accounts at each commerce website that he/she wants the aggregator to access, this is much different than the limitations of claim 1.

Claim 1 recites applying security privileges based on a role-based determination. As pointed out in Applicant's Specification at page 24, lines 10-14, "an example of access privileges being assigned based on user roles is a scenario wherein all users of a certain role (e.g., cashiers) are given a same username/password combination that is associated with one set of asset privileges." This is far different than a customer having multiple accounts on a commerce website. Nowhere in Jancula does it teach that security privileges are applied as claimed. It is therefore submitted that for at least these reasons, claim 1 is in form for allowance.

It is further submitted that due at least to dependence upon what is believed to be an allowable independent claim, claims 2-10 and 11 are also in condition for allowance. This is not to say that at least some of the dependent claims do not individually recite limitations that are patentably distinguishable from the cited reference. For example, claim 8 further defines selectively transmitting a certificate as "selectively transmitting a security certificate that contains an embedded indication of the identity of an entity associated with which the user is associated." It is submitted that Jancula does not teach or suggest this limitation. The Office Action cites Jancula at paragraphs 0056-0057 as teaching this limitation, but an entity association is not mentioned in either of these paragraphs. It is submitted that for at least this additional reason, claim 8 is in form for allowance.

Further, claim 11 further defines the claim step of applying a collection of security privileges as "applying access rights based at least in part upon a determination of which roles are assigned to a user account associated with a user." It is respectfully submitted that Jancula also does not teach or suggest this limitation. It is submitted that claim 11 is in allowable form for this additional reason.

CLAIMS 12, 14-17

With the present response, claim 12 has been amended to further define "using the session ticket as an authenticator for subsequent communications with an entity" as being limited to "using the session ticket as a cryptography key for encrypting or decrypting messages." The Office Action on page 6 states that this added limitation is shown in Janula at paragraphs 0062 and 0093 to 0096. An examination of these paragraphs shows that a "ticket" is used in all of these paragraphs. However, none of these paragraphs discuss using the session ticket as a crytopgraphy key for encrypting messages. Although possession of tickets, verification of tickets, and ticket expiration is discussed in these paragraphs, nowhere does Jancula teach or suggest that the ticket is used as a crytography key for encrypting messages. It is respectfully submitted that claim 12 is in form for allowance at least for these reasons. It is also submitted that claims 14-17 are in form for allowance at least due to their dependence upon what is believed to be an

allowable claim. At least some of these dependent claims are also believed to be allowable based on the merit of their own claim limitations.

CLAIMS 18-20

The Office Action on page 3 indicates that claim 18 is anticipated by Jancula. Claim 18 consists of three elements: a client application, an authorization service and a service provider. It is worth noting the functions performed by each component of the claimed system, namely:

1. As claimed, the client application is configured to respond to a user request by retrieving a security certificate that contains a public encryption key, and by obtaining a service identifier that corresponds to the user request.
2. As claimed, the authorization server is configured to receive the security certificate and the service identifier from the client application and is further configured to selectively generate a corresponding session ticket that is encrypted with a public key.
3. The client application is also configured to receive and decrypt the corresponding session ticket with a private key that corresponds to the public key.
4. As claimed, the service provider is configured to receive a service command with the corresponding session ticket after it has been decrypted by the client application. The service provider is also configured to validate information contained in the corresponding session ticket and selectively execute the service command.

Notably, in accordance with the language of claim 18, **the system component that generates the ticket (i.e., the authentication server) is not the same system component that ultimately executes the service command (i.e., the service provider)**. In contrast, in accordance with the teachings of Jancula, a single system component (i.e., the commerce website) both generates a ticket and, ultimately, provides the access and information.

Further, in accordance with the language of claim 18, **the system component that generates the ticket (i.e., the authentication server) is not the same system component that validates the ticket (i.e., the service provider).** In contrast, in accordance with the teachings of Jancula, a single system component (i.e., the commerce website) both generates a ticket and, ultimately, validates the ticket.

In Jancula, the commerce website creates a new ticket, which is merely a document with data fields for items on the ticket (Jancula, paragraph 0085). In paragraph 0088, the ticket that was created by the commerce website is forwarded to the aggregator for approval by the customer and decryption. After several steps, the aggregator sends a copy of the ticket back to the commerce web site (Fig. 2B). Paragraph 0095 discusses that the commercial website verifies the validity of a ticket in order to authenticate an aggregator's access to a customer's data. This verification ticket includes checking the digital signatures on the ticket against digital certificates maintained within a public key infrastructure. The signatures help ensure the authenticity of the ticket and that the ticket has not been tampered with. Thus, the commerce website both creates the ticket and verifies the validity of the ticket. The commerce website is ultimately also the system component that provides the access/information.

It is therefore submitted that claim 18 is patentable over the prior art for at least these reasons. It is also submitted that claims 19 and 20 are in form for allowance at least due to their dependence upon what is believed to be an allowable claim. At least some of these dependent claims are also believed to be allowable based on the merit of their own claim limitations.

CLAIMS 21-25

Claim 21 is directed to a method for enabling secured communication between a service provider and a plurality of socket applications installed on multiple computing devices within a local access network. As claimed, the service provider is configured to extend a functionality of the socket applications by providing services.

The Jancula reference has nothing, whatsoever, to do with activating socket applications located on computers within a local access network. The purpose of the teachings of the Jancula reference is to provide a way to aggregate information from Internet-deployed e-commerce web sites. The reference has nothing, whatsoever, to do with activating socket applications to receive an extended functionality as claimed.

Further, claim 21 includes a single system component, namely, a centralized authentication service, that does all of: 1) facilitates creation of an account by handling a registration process; 2) receives a public key and an indication of the account; and 3) provides a security certificate that includes the public key. The Jancula reference fails to provide a single system component that performs all of these functions as claimed. Accordingly, it is respectfully submitted that claim 21 is in allowable form for at least these reasons. It is also submitted that claims 22-25 are in form for allowance at least due to their dependence upon what is believed to be an allowable claim. At least some of these dependent claims are also believed to be allowable based on the merit of their own claim limitations.

CLAIMS 26-29

Independent claim 26 recites a method for enhancing the security of communication over a network between multiple peer application hosts. The method includes generating a session ticket. Ultimately, the session ticket is **the session ticket is utilized to at least partially encrypt a message. Following encryption with the session ticket, the message is encrypted with the public key.**

In response to these limitations, the Examiner points to the Jancula reference at paragraphs 0091 to 0096. However, these paragraphs do not teach nor suggest that a message should be at least partially encrypted in accordance with a session ticket. Although these paragraphs do discuss using a ticket of sorts, none of them discuss at least partially encrypting a message prior to encryption of the message with a public key as claimed. In fact, Jancula does not even teach using a session ticket to encrypt a message. It is therefore respectfully submitted that claim 26 is in form for allowance. It is also submitted that claims 27-29 are in form for

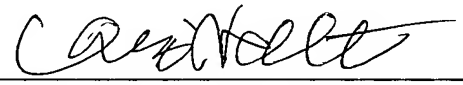
allowance at least due to their dependence upon what is believed to be an allowable claim. At least some of these dependent claims are also believed to be allowable based on the merit of their own claim limitations.

CONCLUSION

Based upon the foregoing, it is respectfully submitted that all claims are in form for allowance based upon the reasons stated above and their dependent nature. The Director is authorized to charge any fee deficiency required by this paper or credit any overpayment to Deposit Account No. 23-1123.

Respectfully submitted,

WESTMAN, CHAMPLIN & KELLY, P.A.

By: 

Christopher L. Holt, Reg. No. 45,844
900 Second Avenue South, Suite 1400
Minneapolis, Minnesota 55402-3319
Phone: (612) 334-3222 Fax: (612) 334-3312

CLH:SD:rkp